

# Googles Cloud-Angebot – Wie wertvoll ist uns der Datenschutz? (Teil 1) **In der Cloud, aber nicht anonym!**

**Bekannt wurde das US-amerikanische Unternehmen Google durch seine gleichnamige Suchmaschine – doch mittlerweile bietet Google viel mehr als das. Google ist ein Internet-Konzern, der in vielen Geschäftsfeldern aktiv ist und immer wieder innovative Produkte und Dienste auf den Markt bringt. Google ist in fast allen Sparten tätig und macht sich mit über einhundert verschiedenen Diensten im Internet breit. Dazu zählen Betriebssysteme, Office-Tools, ein Webbrowser und diverse Plattformen für Kommunikation, Kollaboration, Multimedia, Organisation und Softwareentwicklung sowie Technologien für das Einstellen und Finden von Inhalten. Auch beim Cloud-Computing setzt Google Akzente und wirkt beispielsweise mit Google Chrome OS als Cloud-Client wie ein Innovationsmotor. Im SaaS-Bereich spielt Google mit seinen vielen Diensten eine wichtige Rolle. Außerdem mischt Google mit der App Engine beim PaaS-Angebot mit.**

Wie erfolgreich Google mit seiner Strategie ist, zeigen beeindruckende Zahlen: Im Jahr 2010 war Google mit 114,3 Milliarden US-Dollar Markenwert vor IBM, Apple und Microsoft die mit Abstand wertvollste Marke der Welt. Ein Jahr zuvor setzte der Konzern 24 Milliarden US-Dollar um und verzeichnete dabei einen Gewinn von 6,5 Milliarden US-Dollar. Das entspricht einem Umsatz von ca. 1,34 Millionen US-Dollar pro Mitarbeiter. Damit setzt ein Google-Mitarbeiter durchschnittlich in etwa doppelt so viel um, wie ein Microsoft-Mitarbeiter.

## **Googles Geschäftsmodell – Wir bezahlen mit persönlichen Daten**

Google finanziert sich mit einem Umsatzanteil von 97 Prozent fast ausschließlich über Werbeeinnahmen. Die dazugehörigen Werbeprogramme heißen AdWords und DoubleClick. Dabei können Werbetreibende Anzeigen auf Webseiten von Google und deren Partnern schalten. Diese Werbeanzeigen werden dann den Internet-Nutzern präsentiert und haben dabei zwei Besonderheiten: Zum einen sind die Werbeeinhalte passend auf Nutzer und Situation abgestimmt – man spricht hier von Kontextsensitivität. Zum anderen sind die Anzeigen prinzipiell schlicht und dezent aufgemacht und platziert.

Kontextsensitive Werbung soll inhaltlich passende Werbung für den richtigen Nutzer in der perfekten Situation, sprich an der richtigen Stelle und zur richtigen Zeit anzeigen. Damit das gelingt, zeichnet Google das Verhalten der Internet-Nutzer auf und

verknüpft die erhobenen Daten zu entsprechenden Profilen. Auf diesem Wege analysiert und bewertet Google seine Nutzer und zieht daraus Rückschlüsse, welche Werbung relevant sein könnte. Interessensbasierte und standortbasierte Werbung sind zwei Beispiele für kontextsensitive Werbung. Bei der interessensbasierten Werbung leitet Google die Interessen der Internet-Nutzer aus deren Verhalten ab: Wonach gesucht wird, auf welche Suchergebnisse man klickt, welche Webseiten abgerufen werden usw. Solche persönlichen Daten werden dienstübergreifend erfasst.

Bei standortbasierter Werbung ist der Aufenthaltsort des Internet-Nutzers von zentraler Bedeutung. Wenn Google weiß, wo sich der Nutzer aufhält, können nicht nur Anzeigen für Markenprodukte, Imagewerbung und Onlineshops, sondern auch für Werbetreibende direkt vor Ort geschaltet werden. Standortbezogene Informationen erfasst Google vor allem mit seinem mobilen Betriebssystem Android und den darauf basierenden Anwendungen wie Goggles, Latitude, Navigation oder Near Me Now. Dazu wird das Smartphone des Nutzers geortet, was per GSM-Zelle, GPS oder WLAN während der Nutzung der Dienste geschieht. Als Google-Autos durch die Städte fahren und Aufnahmen für Street View gemacht haben, wurden alle sichtbaren WLAN-Netze samt SSID und MAC-Adresse gleich mitgescannt. Da diese mit Koordinaten verknüpft wurden, war es von nun an möglich, sämtliche Endgeräte, die über einen WLAN-Zugang verfügen, zu orten. Das bedeutet, Google führt eine Liste aller

WLANs einschließlich der Information, wo diese stehen. Android-Handys dienen dann als Sensoren, die je nach Konfiguration des Smartphones ständig GSM-Zell-Informationen sowie GPS- und WLAN-Messdaten nach „oben“ senden. Googles Geolocation API, die unter anderem Zugriffe auf die WLAN-Datenbank ermöglicht, erlaubt es sogar, jedes Endgerät, das über einen WLAN-Zugang verfügt, zu orten. Dazu werden lediglich die entsprechenden Messdaten benötigt, die beispielsweise der Webbrowser oder die Google Toolbar auslesen können.

Google geht beim Erfassen von Daten so eifrig vor, dass es sich den Ruf als sammelwütiger Datenkraken eingehandelt hat. Kritik von Daten- und Verbraucherschützern sowie anderen bezieht sich hier insbesondere auf die persönlichen Daten, denn die Privatsphäre der Internet-Nutzer und ihr Recht auf informationelle Selbstbestimmung sind massiv gefährdet. Das Recht auf informationelle Selbstbestimmung 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. Somit soll der Einzelne vor der Beeinträchtigung beziehungsweise unerwünschten Folgen, insbesondere durch zweckwidrigen Missbrauch, beim Umgang mit seinen persönlichen Daten geschützt werden.

## **Google Apps – Das SaaS-Paket von Google**

Google Apps ist ein Softwarepaket, das zwar von Google gehostet wird, jedoch unter einem eigenen Domainnamen erreichbar ist und vornehmlich für Unternehmen und andere Organisationen geschnürt wurde. Über eine Administrationsoberfläche kann das Unternehmen die Plattform dann samt Nutzer, Rollen und Dienste selbst verwalten. Dabei kann beispielsweise definiert werden, welche Google-Dienste von welchen Mitarbeitern genutzt werden dürfen. Anfangs war Google Apps mehr oder weniger nur eine Plattform für Messaging und

Kollaboration und somit ein Konkurrent zu Produkten wie Microsoft Exchange und Lotus Notes. Mittlerweile sind etliche Dienste dazugekommen, sodass das SaaS-Paket nun mehr als 30 Google-Dienste umfasst.



Google Apps  
(<http://www.digitaltrends.com/computing/gsa-picks-google-apps-microsoft-retorts/>)

Es stehen prinzipiell zwei Versionen von Google Apps zur Verfügung: Eine kostenlose, die auf 50 Endnutzer limitiert ist, und eine kostenpflichtige, für die 40 Euro jährliche Kosten pro Endnutzer anfallen. Für Bildungs- und Regierungseinrichtungen sowie für gemeinnützige Organisationen gelten gesonderte Konditionen. Endnutzer sind die Mitarbeiter der jeweiligen Organisation. Bei der kostenpflichtigen Version stehen außerdem weitere Features wie mobile Zugriffsmöglichkeiten, 25 GByte E-Mail-Speicherplatz pro Endnutzer, Interoperabilität zu Microsoft Outlook und anderen Anwendungen sowie zusätzliche Sicherheitskonzepte (erzwungene Verschlüsselung, Richtlinien für Passwörter etc.) zur Verfügung. Zudem umfasst die Nutzungsvereinbarung der kostenpflichtigen Version sowohl ein Service-Level-Agreement, das 99,9 Prozent Verfügbarkeit garantiert, als auch einen 24/7 Support. Ein weiterer wichtiger Unterschied zur kostenlosen Version ist, dass Werbeanzeigen standardmäßig deaktiviert sind.

### Das Datenschutz-Risiko – Die Nutzer-Perspektive

Bei der Nutzung von Googles Internet-Angeboten entsteht ein Datenschutzrisiko, das sich auf die persönlichen Daten der

Nutzer beziehungsweise Endnutzer bezieht. Bei den Diensten von Google Apps handelt es sich fast ausschließlich um solche, die auch jeder Privatanwender mit einem normalen Google-Konto nutzen kann. Dementsprechend sind sowohl herkömmliche Internet-Nutzer als auch die Mitarbeiter der Unternehmen, die Google Apps im Einsatz haben, betroffen. Im Folgenden soll betrachtet werden, welche persönlichen Daten Google wo verarbeitet und warum das ein Risiko für Internet-Nutzer darstellt.

Für kontextsensitive Werbung benötigt Google Profile der Internet-Nutzer. Diese Nutzerprofile entstehen, da persönliche Daten im Google-Konto zusammenlaufen. Dieses Google-Konto wird für viele Dienste, manchmal aber auch nur für bestimmte Funktionalitäten innerhalb der Dienste benötigt. Diese stehen dem Nutzer dann erst nach einem erfolgreichen Login zur Verfügung. Einige der persönlichen Daten, die im Google-Konto gespeichert werden, gibt man freiwillig preis, indem man selbst aktiv wird und diese zum Beispiel in entsprechende Formularfelder einträgt. Dazu zählt die Angabe von Namen, Anschriften und beruflichen Laufbahnen in diversen Profilen verschiedener Dienste oder von Kontoverbindungen bei Adwords oder Google Checkout. Auch Content, der bewusst ins Internet gestellt wird, ist mit dem Google-Konto verknüpft. Beispiele für Content sind Blogs bei Blogger.com sowie Dokumente, Bilder und Videos, die beim Office-Tool Google Docs, beim sozialen Netzwerk Orkut, bei den Picasa Webalben oder bei YouTube hochgeladen werden. Dazu kommen persönliche Daten, die automatisch bei der Nutzung der Dienste verarbeitet und deshalb eher unbewusst mit dem Google-Konto verknüpft werden: Berechnete Routen in Google Maps oder Suchanfragen im Webprotokoll, aber auch Kontakte in Orkut oder Gmail und Kommunikationsinhalte in Gmail, Google Talk oder Google Voice. Das Webprotokoll ist Teil des Google-Kontos und zeichnet Suchanfragen dienstübergreifend auf.

Weitere persönliche Daten wie Anfragen und abgerufene Inhalte werden ebenfalls dienstübergreifend erfasst und unabhängig von der Nutzung eines Google-Kontos in sogenannten Protokolldateien gespeichert. In diesen Dateien wird also das Verhalten eines Internet-Nutzers aufgezeich-

net, indem Webanfragen (HTTP-Request) und –antworten (HTTP-Response) bei der Kommunikation mit Google aufgezeichnet werden. Unter den erfassten Daten sind Suchanfragen, angeklickte Suchergebnisse, abgerufene Webseiten etc. Um diese einem bestimmten Internet-Nutzer zuzuordnen, werden die persönlichen Daten unter entsprechenden Identifikations- beziehungsweise Wiedererkennungsmerkmalen erhoben und abgespeichert. Dazu gehören insbesondere Cookies und IP-Adressen. Daneben bietet sich auch eine Browser-ID zur Identifikation von Internet-Nutzern an – Google Chrome zum Beispiel verfügt über eine solche eindeutige Installationskennung. Wie dem Namen zu entnehmen ist, identifiziert die ID eine spezielle Installation des Chrome-Browsers auf dem Rechner des Internet-Nutzers und kann den Browser so immer wiedererkennen. Cookies, IP-Adressen und Browser-IDs als technische Identifikationsmerkmale ermöglichen Google eine Verknüpfung beziehungsweise Korrelation von persönlichen Daten zu Nutzerprofilen.

Infolge des Google-Kontos und der Protokolldateien entstehen ausführliche Nutzerbeziehungsweise Persönlichkeitsprofile. Diese lagern auf Google-Servern und sind dort generell nicht hundertprozentig vor Datenmissbrauch und eigens von Google verursachten Datenschutzpannen geschützt. Auch vor gerichtlichen Zugriffen sind diese Persönlichkeitsprofile nicht gesichert. Die Möglichkeit der dienstübergreifenden Verknüpfung und Korrelation von persönlichen Daten verschärft das Problem erheblich. Diesbezüglich nimmt Google eine Sonderstellung ein, denn Google hat über einhundert Dienste, die fast sämtliche Bereiche abdecken und bei denen gemäß Single Sign-on ein einziges Google-Konto verwendet werden kann. Es gibt wohl kein Unternehmen, das sich diesbezüglich im Internet so breit macht und zugleich aufgrund des Geschäftsmodells auf persönliche Daten angewiesen ist wie kein anderer. Zu den allgemeinen Risiken, die mit Persönlichkeitsprofilen im Internet verbunden sind, gehören zusätzlich Identitätsdiebstähle (vor allem, um Kriminaltaten unter vorgetäuschter Identität auszuüben), Belästigungen (zum Beispiel durch Werbetreibende oder Personalvermittler), Verfolgungen (zum Beispiel Rasterfahndungen oder Stalking), Demütigungen (Stichwort „Cy-

ber-Mobbing“) und verzerrte Persönlichkeitsbilder (Google und andere, die elektronisch Daten erfassen und verknüpfen, unterscheiden nicht zwischen richtigen und falschen Informationen).

## Google speichert Kommunikationsdaten

In verschiedenen Diensten werden Kommunikationsdaten verarbeitet und mit dem Google-Konto verknüpft. Google liest sogar Kommunikationsinhalte, um dann kontextsensitive Werbung zu schalten. Bei der kostenpflichtigen Version von Google Apps werden allerdings keine Kommunikationsinhalte gelesen und ausgewertet, da Google Apps in dieser Version standardmäßig frei von Werbung ist. Gmail ist ein hervorragender E-Mail-Dienst, bei dem jedoch E-Mails und Kontakte im Google-Konto gespeichert werden. Die Inhalte der E-Mails werden durchsucht und analysiert, um inhaltlich relevante Werbung zu platzieren.



Kontextsensitive Werbung bei Gmail  
(Quelle: [de.wikipedia.org/Google\\_Mail](http://de.wikipedia.org/Google_Mail))

Google Talk ist ein Instant Messenger, der in mehrere andere Google-Dienste integriert ist. Bei Talk erfasst Google Daten über die Zeitpunkte der Verwendung, die Anzahl der Kontakte, die Kontakte mit denen man kommuniziert und die Häufigkeit sowie das Volumen von Datentransfers. Außerdem werden alle Konversationen von Google mitgelesen und gespeichert. Auch diese werden automatisch durchsucht und ausgewertet, um kontextsensitive Werbung zu platzieren. Ähnlich problematisch sieht es bei der SMS-Versendung per Google Talk aus. Wird dieses Feature genutzt, werden die Telefonnummer des Empfängers, der Inhalt der SMS und die Kommunikationszeiten aufgezeichnet. All diese persönlichen Daten sind mit dem Google-Konto verknüpft. Bei Google Voice, einem webbasierten Telefonmanager, der bisweilen nur in den USA verfügbar ist, werden Telefongespräche nach einer automatischen Spracherkennung aufgezeichnet und mit dem Google-Konto verknüpft.

Google Groups ist ein Dienst, der genutzt werden kann, um Diskussionsgruppen zu bestimmten Themen zu gründen und bestehenden Gruppen beizutreten. Teilnehmer einer Gruppe können so per Internet über bestimmte Themen in Foren diskutieren. Inhalte werden je nach Konfiguration für die Websuche verfügbar gemacht. Beiträge können nicht anonym verfasst werden und sind daher stets mit dem Google-Konto des Verfassers verknüpft. Auch im sozialen Netzwerk Orkut werden Kontakte und Nachrichten, aber auch weitere persönliche Daten mit dem Google-Konto verknüpft. Mit Buzz verfügt Google über ein weiteres soziales Netzwerk. Soziale Netzwerke sind datenschutzrechtlich generell eine Herausforderung, denn Internet-Nutzer geben hier tendenziell sehr viele persönliche Daten preis.

## Google ist ein Content-Provider

Auch Inhalte beziehungsweise Content, der bei Google-Diensten hochgeladen wird, ist fortan im Google-Konto gespeichert. Bei Blogger.com zum Beispiel werden eigene Beiträge, Bilder und Kommentare mit dem Google-Konto verknüpft. Darüber hinaus wird bei der Verwendung von Blogger Mobile die Handynummer mit dem Google-Konto verknüpft, sofern man einen Beitrag per SMS oder MMS absendet. Knol ist eine Wissensdatenbank, die Wikipedia ähnelt, denn hier sollen Artikel zu verschiedenen Themen behandelt werden. Im Unterschied zu Wikipedia können jedoch mehrere Autoren mehrere Artikel zum gleichen Thema verfassen. Eine Bewertung durch andere Nutzer bestimmt die Relevanz und somit auch das Ranking in Suchergebnissen. Somit ist Knol keine klassische Enzyklopädie. Artikel von Autoren sowie abgegebene Kommentare und weitere persönliche Daten laufen im Google-Konto zusammen. Weitere Beispiele für Dienste, in denen Google den Content seiner Nutzer mit dem Google-Konto verknüpft, sind Fotos bei den Picasa Webalben, Dokumente bei Google Docs und Videos bei YouTube. Bei YouTube wird außerdem das Verhalten der Nutzer im Dienst aufgezeichnet. Dazu zählen zum Beispiel die Videos, die man sich anschaut

oder auch die letzten Aktivitäten wie Videos mögen, kommentieren oder sie den Favoriten hinzuzufügen.

## Google erfasst sensible Daten

Neben Content und Kommunikationsdaten gibt es weitere persönliche Daten, die in diversen Diensten erfasst und mit dem Google-Konto verknüpft werden. Der Online-Bezahldienst Google Checkout zum Beispiel setzt die Angabe persönlicher Informationen voraus, die von Google auf Korrektheit überprüft werden: Vor- und Nachname, Anschrift, Telefonnummer, E-Mail-Adresse sowie Kreditkartennummer beziehungsweise Bankverbindung. Außerdem werden transaktionsbezogene Daten gespeichert. Dazu zählen der Transaktionsbetrag, eine Beschreibung der Ware oder der Dienstleistung, die Namen von Käufer und Verkäufer und die verwendete Zahlungsart. Bei Google Finance können eigene Finanzportfolios verwaltet und ausgewertet werden. Solche Portfolios erlauben unter anderem die Zusammenstellung eigener Wertpapiere in bestimmten Stückzahlen einschließlich der Verwaltung von Transaktionen. Portfolios wiederum werden im Google-Konto gespeichert. Der Kalender-Dienst erlaubt das Verwalten von Terminen einschließlich der Teilnehmer, die über deren Google-Konto mit den Terminen verknüpft werden können. Somit weiß Google fortan, mit wem man sich wann und wo trifft beziehungsweise treffen wird oder getroffen hat.

Wie bei den Protokolldateien erwähnt, zeichnet Google sämtliche Anfragen auf, um Interessensprofile abzuleiten, die wiederum dazu dienen, interessensbasierte Werbung zu platzieren. Wenn das Webprotokoll aktiviert und man eingeloggt ist, werden solche Daten teilweise sogar mit dem Google-Konto verknüpft. Das betrifft nicht nur die Websuche sondern auch andere Suchen in weiteren Diensten. Im Rahmen von Google Apps wird eine angepasste Suche angeboten. Sofern die Endnutzer diese Google-Suche verwenden, konzentrieren sich hier die Suchanfragen der Mitarbeiter. Bei Google Maps kann der eigene



Für Abonnenten ist dieser Artikel auch digital auf [www.datakontext.com](http://www.datakontext.com) verfügbar



Weitere Artikel/News zum Schwerpunkt unter [www.datakontext.com/cloud](http://www.datakontext.com/cloud)

Standort festgelegt und berechnete Routen mit dem Google-Konto verknüpft werden.

Google Chrome OS ist ein kostenloses Betriebssystem, das auf dem gleichnamigen Webbrowser Google Chrome basiert. Die Grundidee ist die folgende: Wenn nur noch auf SaaS-Angebote und nicht mehr auf lokale Softwareinstallationen zugegriffen wird, reicht ein Webbrowser eigentlich vollkommen aus. Da jedoch auch ein Webbrowser eine Laufzeitumgebung benötigt, hat Google seinen Chrome-Browser mit einem Linux-Kernel versehen. Auch Google Chrome sammelt fleißig persönliche Daten: Erfasst werden URLs oder Suchanfragen, und zwar von der Eingabe des ersten Zeichens des entsprechenden Suchbegriffs beziehungsweise der URL, bis zum Absenden der Anfrage. Auch Nutzungsstatistiken (zum Beispiel Informationen zu den Browser-Einstellungen, zu den Klicks auf Schaltflächen oder zur Speicherauslastung) werden an Google gesendet. Bei Nutzung der Synchronisierungsfunktion werden Browsereinstellungsinformationen (zum Beispiel Lesezeichen) mit dem Google-Konto verknüpft und auf Google-Servern gespeichert. Bei der Installation der Google Toolbar werden solche persönlichen Daten übrigens auch bei der Verwendung anderer Webbrowser an Google übertragen. Dabei arbeitet die Toolbar wie ein Sensor, der Internet-Nutzer in großer Zahl erreicht und daher ein wichtiges Instrument für Google darstellt, um viele Nutzerdaten zu sammeln.

Außerdem verfügt Google über viele weitere Dienste, die ebenfalls persönliche Daten verarbeiten. Dazu gehören beispielsweise die mobilen Dienste oder Google Health. Bei Health werden Gesundheitsdaten wie Krankheiten, Therapien und sogar die eigene DNS mit dem Google-Konto verknüpft.

### Das Datenschutz-Risiko – Die Unternehmer-Perspektive

Nach der Betrachtung der Datenschutzrisiken aus Sicht der Internet-Nutzer bleibt festzustellen, dass durchaus ausführliche Persönlichkeitsprofile auf den Servern von Google entstehen können. Bei Google Apps weitet sich das Datenschutzrisiko auf Unternehmensdaten aus, denn fast alle zuvor betrachteten Dienste sind Teil von Google Apps. Chrome OS gehört natürlich nicht

dazu. Aber auch hier setzt sich Google dafür ein, dass Unternehmen das Betriebssystem künftig als Cloud-Client einsetzen. Aus Sicht eines Unternehmens handelt es sich bei den von Google verarbeiteten Kommunikationsdaten, Inhalten wie Dokumente und weiteren Daten nun um unternehmensinterne Daten, also Unternehmenswerte. All diese Daten, mit denen die Mitarbeiter des Unternehmens arbeiten, laufen auf der Google Apps-Plattform zusammen. Folgerichtig entstehen Unternehmensprofile auf den Servern von Google.

Problematisch ist auch, dass die Bestimmungen zur Nutzung von Google Apps auf einer 18-seitigen Vereinbarung von Google diktiert werden. Es gibt keinen Verhandlungsspielraum – entweder man akzeptiert Googles Bedingungen oder nicht. Die Vereinbarung kann jederzeit aktualisiert werden und es liegt in der Verantwortung des Unternehmens, diese Vereinbarung in regelmäßigen Abständen auf Aktualisierungen zu überprüfen. In der Vereinbarung wird zudem sowohl auf die Gültigkeit der allgemeinen als auch dienstspezifischen Nutzungs- und Datenschutzbedingungen hingewiesen. Bei den vielen Diensten entsteht ein komplexes Geflecht aus verschiedenen Bedingungen und Richtlinien. Transparenz sieht anders aus!

Hinzu kommen laut Vereinbarung weitere Punkte: Von Google erfasste Informationen können in den USA und in jedem anderen Land, in dem Google oder Auftragnehmer von Google Niederlassungen haben, gespeichert und verarbeitet werden. Das Unternehmen stimmt jeglichen anwendbaren Gesetzen und Bestimmungen zur Steuerung des Datentransfers zu, einschließlich der Export Administration Regulations des US-Handelsministeriums und der Trade and Economic Sanctions des Amts für ausländische Vermögenskontrolle des US-Finanzministeriums. Außerdem unterliegt die Vereinbarung den gesetzlichen Bestimmungen des Staates Kalifornien und den dort geltenden Bundesgesetzen der USA. Gerichtsstand ist der kalifornische Verwaltungsbezirk Santa Clara. Außerdem finden die Konventionen der Vereinten Nationen zu Verträgen für den internationalen Verkauf von Produkten sowie das Gesetz zur Vereinbarung von Transaktionen mit Computerinformation ausdrücklich keine Anwendung auf die Vereinbarung. Ob ein

Unternehmen solchen Bedingungen zustimmen und Google unternehmensinterne Daten anvertrauen sollte, muss genau geprüft werden. Bedacht werden sollte auch, dass Google generell nicht davor zurückschreckt, E-Mails, Telefonate und Chatgespräche seiner „Kunden“ für Werbezwecke zu durchsuchen – zumindest sofern man die kostenlose Version von Google Apps nutzt oder Werbung bei der kostenpflichtigen Version aktiviert hat. Generell hat Google hier nichts verloren! ■

Im zweiten Teil dreht sich alles um die Frage, wie das Sammeln und Verknüpfen von persönlichen Daten von Internet-Nutzern bei Google reglementiert werden kann.

Weitergehende Informationen und Quellenangaben sind in der Studie, zu der dieser Artikel verfasst wurde, zu finden: <http://www.internet-sicherheit.de/fileadmin/docs/publikationen/2011/Google-StudieV2.0.pdf>



Nikolai Spogahn

Norbert Pohlmann