Wie man Googles Dienste umsichtig nutzt

Bauchladen

Nikolai Spogahn, Norbert Pohlmann

Für kontextsensitive Werbung braucht Google persönliche Daten, die die Firma aus vielen Diensten, die sie anbietet, zieht. Um nicht ein Übermaß an Informationen preiszugeben, müssen Anwender findig sein.

Außer der Suchmaschine bietet Google Office-Programme, einen Webbrowser sowie diverse Plattformen für Kommunikation, Kollaboration, Multimedia, Organisation und Softwareentwicklung. Im Angebot befinden sich Dienste wie Location-based Services rund um Karten, Navigation, Routenplaner, Street View, Satellitenbilder oder Medienverzeichnisse wie Books und YouTube. Dazu kommen das mobile Betriebssystem Android, der Cloud-Client Chrome OS und so weiter. Das Angebot ist zum Großteil kostenlos.

Bei kontextbezogener Werbung ist Google Vorreiter und Marktführer. Zu solcher Werbung zählt beispielsweise die interessenbasierte, bei der Nutzer auf ihre Interessen zugeschnittene Anzeigen präsentiert bekommen. Ortsbezogene beziehungsweise mobile Werbung geht einen Schritt weiter. Dafür verknüpft die Firma persönliche Daten zu Profilen, die das Anwenderverhalten widerspiegeln sollen, und diese mit dem Aufenthaltsort des Geräts.

Wer diese Dienste nutzt, geht im schlimmsten Fall das Risiko ein, seine Privatsphäre aufzugeben. Auf der einen Seite laufen persönliche Informationen im Google-Konto zusammen, das für viele Dienste, manchmal aber nur für bestimmte Funktionen innerhalb der jeweiligen Dienste erforderlich ist. Diese stehen erst nach dem Login zur Verfügung. Bei den gespeicherten persönlichen Daten kann man zwischen direkt und indirekt erfassten unterscheiden. Direkt, wenn der Surfer sie bewusst angibt, indem er sie in Formularfelder einträgt oder Dateien hochlädt. Dazu kommen indirekt und (vermutlich) für den Nutzer ungewollt erfasste persönliche Daten: sein während der Dienstnutzung aufgezeichnetes Verhalten, zu dem Suchanfragen, Routen oder Kontakte zählen.

Weitere Informationen wie HTTP-Anfragen, Suchergebnisse und abgerufene Inhalte erfasst Google ebenfalls dienstübergreifend und speichert sie unabhängig von der Nutzung eines Kontos in sogenannten Protokolldateien. Um diese einem bestimmten Nutzer zuzuordnen, erheben und speichern die Kalifornier die persönlichen Daten unter Identifikations- beziehungsweise Wiedererkennungsmerkmalen: Cookies und IP-Adressen, wobei die Zuordnung vom Surfer zur IP-Adresse nicht so konsistent ist wie bei einem Cookie, denn IP-Adressen vergeben Provider in der Regel dynamisch.

Circa 80 Prozent der meistbesuchten deutschen Webseitenbetreiber sollen im Jahr 2008 Google Analytics eingesetzt haben (nach Spiegel Online, siehe *iX*-Link). Google speichert das Verhalten der Besucher dieser Webseiten auf seinen eigenen Servern. Daten, die Aufschluss über die Interessen von Nutzern geben können, werden nicht nur über die Suche und Googles Analytics erfasst, sondern beispielsweise auch in den sozialen Netzen Buzz oder Orkut, über mit Gmail gesendete und empfangene E-Mails oder über Checkout, den Bezahldienst, dessen Transaktionen dauerhaft im Google-Konto landen. Entscheidet man sich für die Nutzung von Gmail, liest und analysiert Google alle privaten E-Mails, um anschließend inhaltlich relevante Werbung schalten zu können.

Ortsbezogene Informationen laufen in der Geolocation-API zusammen, die Schnittstellen anbietet, um beispielsweise zu einer MAC-Adresse einschließlich SSID und Signalstärke die Koordinaten zu liefern. Das befähigt Google, sogar ohne GPS und Mobilfunkempfang jeden Internetnutzer zu orten, dessen WLAN-Funktion aktiviert ist.

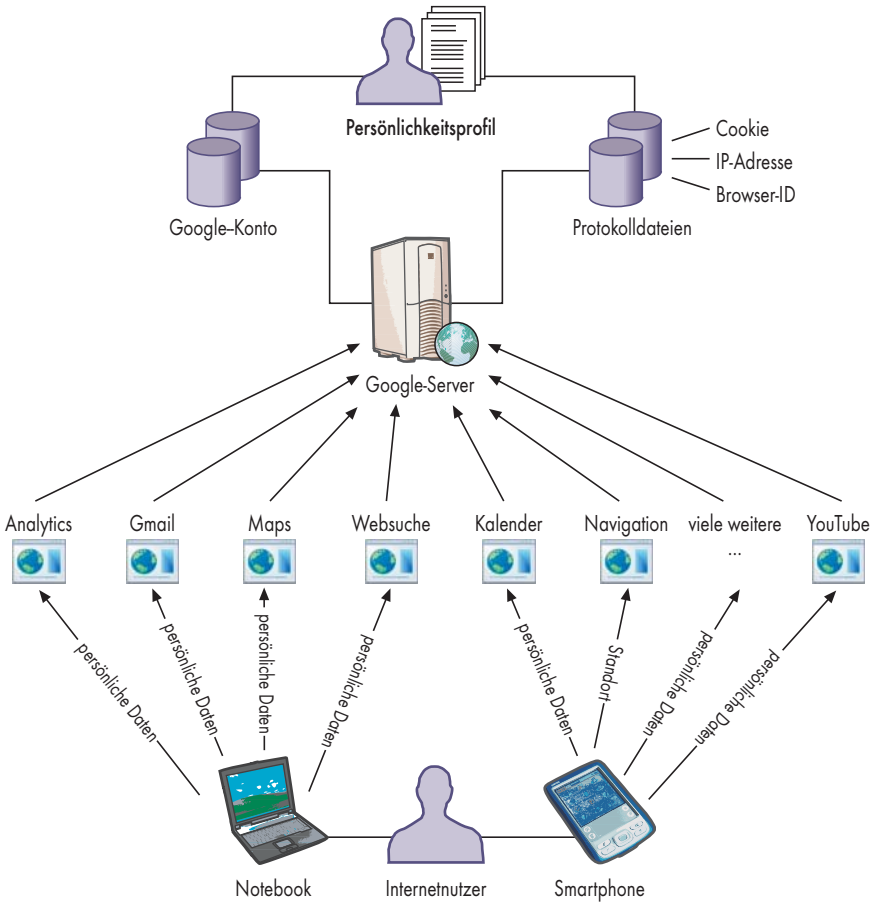
Nicht identifizierende Angaben

Bei der Fülle an erfassten und verknüpften Daten kommt die Frage auf, was Anwender unternehmen können, um sie zu schützen. Das Konto ist der erste Ansatz, denn hier können Nutzer

Verknüpfungen und somit ausführliche Persönlichkeitsprofile zumindest teilweise verhindern. Zunächst bietet es sich an, nur nicht identifizierende Angaben zu machen (exklusive Name, Anschrift, Bankverbindung, Lebenslauf et cetera). Auf Dienste, bei denen diesbezüglich korrekte Angaben Pflicht sind (Checkout, Health) oder bei denen man tendenziell viele persönliche Daten preisgeben müsste (Buzz, Orkut), sollte man verzichten und nach Alternativen suchen – oder ein separates Konto verwenden.

Picasa etwa gruppiert alle auf Bildern erkannte Personen und kann ihnen zur Indizierung einen Namen zuweisen. Sofern man sich bei dieser herunterladbaren Software mit dem Google-Konto anmeldet, kann man dafür die Kontakte aus dem Konto verwenden – oder Bilder in Picasa-Webalben hochladen und diese mit Offline-Bildern synchronisieren.

Beim Einrichten eines Kontos ist standardmäßig die Webhistorie (das „Webprotokoll“) aktiviert. Sowie jemand bei der Nutzung von Suchdiensten eingeloggt ist, speichert Google alle Anfragen in dieser Webhistorie. Neben dem Zugriff auf die eigene Suchhistorie erhalten Anwender mit der Zeit bessere, das heißt personalisierte Suchergebnisse geliefert; das jedenfalls behauptet Google.



Über die vielen Dienste, die Google anbietet, können die Kalifornier dem über ein Cookie oder Ähnliches identifizierten Nutzer ein Profil zuordnen (Abb. 1).

Verzicht auf tolle Features

Android war bis zur Version 1.5 (30. April 2009) nicht ohne Google-Konto verwendbar, seitdem ist das nicht mehr der Fall. Allerdings bedeutet die Nutzung von Android ohne Konto den Verzicht auf tolle Features. Es ist deutlich praktischer, sein Smartphone damit in Betrieb zu nehmen, weil es so beispielsweise Kontakte und Termine aus dem Konto liefert. Der Nutzer muss also abwägen, ob ihm der Schutz seiner Daten oder die Features wichtiger sind.

Wer sich der Verwendung eines Google-Kontos nicht entziehen kann, sollte allerdings darauf achten, dass nicht zu viele persönliche Daten in einem einzigen Konto zusammenlaufen. Benötigt ein Internetnutzer ein professionelles Konto für Blogger.com, Googles Knol und AdWords, sollte er es, weil es ihn zweifelsfrei identifiziert, nicht noch für andere Dienste verwenden, sondern dafür lieber ein zusätzliches, privates und anonymes Konto nutzen. Im Extremfall könnte man sogar pro Dienst, bei dem ein Konto unerlässlich ist, ein gesondertes verwenden.

So viel zum Google-Konto. Um eine Korrelation von auf der Basis von Cookies erhobenen persönlichen Daten zu verhindern, bieten sich Plug-ins für den Webbrowser an. Sie unterbinden Cookies oder löschen sie jedes Mal wieder. Außerdem gibt es Plug-ins, die Google bezüglich der Datensammelei auf andere Art und Weise das Handwerk legen, wie GoogleSharing. Bei diesem Projekt wird ein Proxy-Server zwischen den Internetnutzer und Google geschaltet. Der leitet Suchanfragen und abgerufene Inhalte um und anonymisiert sie dabei. Diese Anonymisierung betrifft Cookies und die IP-Adresse. Google kann in diesem Fall das Verhalten in diversen Google-Diensten nicht mehr einem speziellen Internetnutzer zuordnen, denn der Proxy verschleiert dessen Identität, indem er diese bei jeder Anfrage an Google-Server durch eine neue GoogleSharing-Identität ersetzt. Die vorherige Identität weist er dem nächsten Nutzer zu und so weiter, daher der Name des Projekts.

Google selbst bietet zwei interessante Browser-Erweiterungen an: Das Analytics Opt-out Browser Add-on und das

iX-TRACT

- Google benötigt persönliche Daten der Kunden, um sein Geschäftsmodell der kontextbasierten Werbung umsetzen zu können.
- Zurückhaltung bei der Datenfreigabe in der jeweiligen Konfiguration hilft, die Menge der für Google verwendbaren persönlichen Daten zu begrenzen.
- Wenn viele Daten Voraussetzung für die Teilnahme an einem Dienst sind, sollte man überlegen, diesen mit gesondertem Login zu nutzen.

Plug-in zum Deaktivieren des Cookie für Werbeanzeigen. Das erste teilt laut der Browser-Add-on-Seite „dem JavaScript (*ga.js*) von Google Analytics mit, dass keine Informationen über den Website-Besuch an Google Analytics übermittelt werden sollen“, das zweite ist ein offizielles Plug-in zum dauerhaften Deaktivieren des DoubleClick-Cookie. Beide Plug-ins sind Teil von Googles Opt-out-Strategie.

Datenschutz per Opt-out-Strategie

Ohne Googles Zugriff auf persönliche Daten hätte dessen kontextsensitive Werbung keine Chance, und das Geschäftsmodell könnte nicht funktionieren. Daher hat die Firma sich entschieden, die persönlichen Daten trotz Kritik und Widerstand zum Großteil weiterhin zu erfassen, dem Nutzer jedoch einzuräumen, dies bis zu einem gewissen Grad zu unterbinden – in der stillen Hoffnung, dass wenige Anwender diese Optionen wählen. Diese Bestimmungen dürften allerdings die wenigsten vor dem Nutzen eines Dienstes lesen.

Der Datenschutzproblematik vollständig entzogen hat sich Google mit dieser Opt-out-Strategie allerdings nicht, denn sie ist nicht mit dem Grundsatz „Verbot mit Erlaubnisvorbehalt“ deutscher und europäischer Datenschutzgesetze in Einklang zu bringen. Demnach müssen Internetnutzer explizit in die Erhebung und Verarbeitung ihrer persönlichen Informationen einwilligen, bevor Google diese überhaupt erfassen darf. Daher dürfte das Unternehmen keine Nutzungs- und Datenschutzbestimmungen diktieren, in denen es lediglich allgemein auf die Verarbeitung persönlicher Daten und deren Zwecke sowie die Optionen, diese Verarbeitung zu unterbinden, hinweist.

Zur Gesetzeslage in Deutschland: Das oben genannte Verbot mit Erlaubnisvorbehalt lässt sich unmittelbar aus dem Recht auf informationelle Selbstbestimmung ableiten. Die Erhebung, Verarbeitung oder 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 (siehe [3]).

Anwender müssen selbst für ihren Datenschutz aktiv werden. Google hingegen muss für mehr Transparenz in der Erhebung und Verarbeitung persönlicher Daten sorgen sowie die Schnittstellen zu seinen Diensten deutlicher und einfacher gestalten. Außerdem muss die Firma Nutzern eine Schnittstelle zur Verfügung stellen, die es ihnen ermöglicht, die mit ihrer Person verknüpften Daten im Sinne des Auskunftsrechts zu „sehen“. Googles Dashboard ist ein guter Ansatz; allerdings setzt es das Auskunftsrecht unzureichend um, da es lediglich unmittelbar mit dem Google-Konto verknüpfte Daten anzeigt. Dabei umfasst das Dashboard längst nicht alle persönlichen Daten, die im Konto zusammenlaufen, und schon gar nicht per Cookie und IP-Adressen zu Profilen verknüpfte.

Welche Optionen der Nutzer hat

Außer den erwähnten Browser-Plug-ins hat der Nutzer im Google-Umfeld weitere Optionen, um darüber zu entscheiden, welche Informationen er über sich preisgibt, meist als Teil der Dienstkonfigurationen. So können Anwender in vielen Diensten einstellen, welche Daten übertragen beziehungsweise gespeichert werden und für wen erfasste Daten freigegeben (sichtbar) sind. Solche Optionen sollten sie genau wie Plug-ins in Anspruch nehmen.

Etwa vierzig Dienste hat Nikolai Spogahn daraufhin untersucht, welche Daten im Einzelnen erhoben werden und wie es diesbezüglich mit den Optionen aussieht, um das zu verhindern [1]. Insgesamt boten sich einige solcher Optionen. Wenn beispielsweise jemand auf Blogger.com bloggt, sind standardmäßig dessen Profil und in diesem Dienst verfolgte Webseiten freigegeben. Sofern diese beiden Freigaben nicht jeweils deaktiviert sind, bleiben die Daten für jeden sichtbar.

Bei YouTube erlaubt Google seinen Nutzern, die nicht gerade aussagekräftige Option „Bitte meine Kontodaten verwenden, um mir relevante Werbung zu liefern“ zu deaktivieren. Außerdem werden „Statistiken und Daten“ für eigene Videos standardmäßig öffentlich angezeigt, was man ebenfalls unterbinden kann. Dass alle den YouTube-Kanal sehen können, sofern sie über die E-Mail-Adresse des dazugehörigen Google-Kontos verfügen, kann der Anwender ebenfalls deaktivieren. Manchmal waren die Optionen jedoch unzureichend, sodass man von der Nutzung einiger Dienste nur abraten kann.

Verknüpfung mit dem Konto verhindern

Folgende Details zeigen, wie jeder die Verknüpfung persönlicher Daten mit dem Google-Konto verhindern kann: Bei Googles Talk, dem Instant Messenger, der in mehrere andere Dienste integriert ist, kann man einstellen, dass

Was Google alles über jeden wissen könnte

Nutzte man viele Google-Dienste leichtsinnig, wäre das Datenschutzrisiko groß. Google wüsste in diesem Fall:

– wer man ist und wo man wohnt (Buzz, Checkout, Gmail, Profiles et cetera)

– welche sozialen Kontakte man pflegt (Buzz, Gmail, Orkut, Talk, Voice et cetera)

– wo man sich gerade aufhält (Ortung per GSM-Zelle, GPS oder WLAN bei mobilen Diensten wie Latitude, Navigation oder Near me now; potenziell aber bei allen anderen Endgeräten, die WLAN-Signale empfangen)

– wohin man will (Earth, Maps, Navigation et cetera)

– welche Termine man hat (Kalender, Sync et cetera)

– 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 lautet (Checkout)

– wer die Partner bei 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)

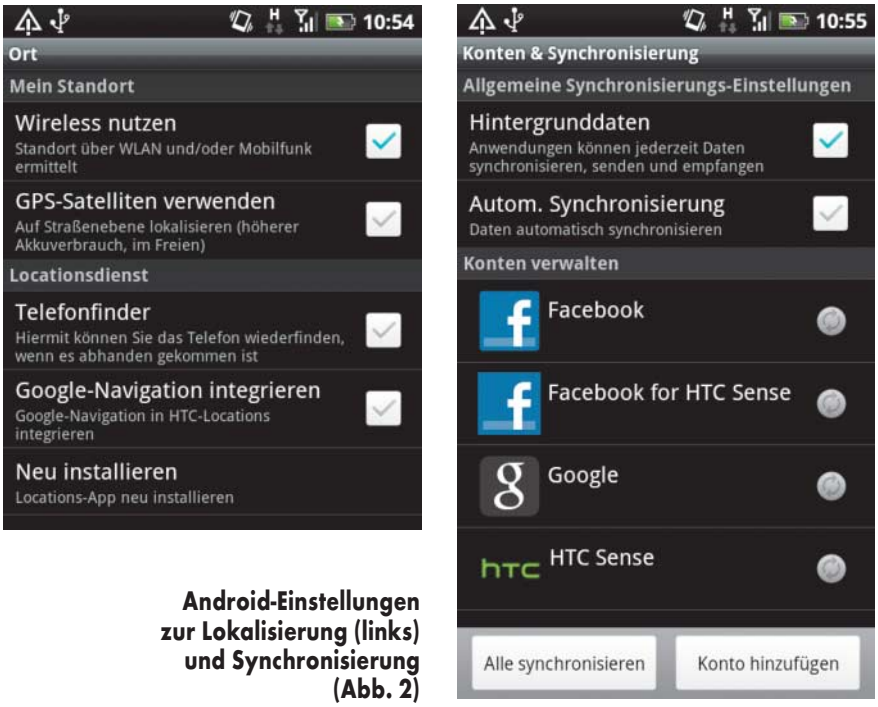
– wie man aussieht (Buzz, Gmail, Picasa, Profiles et cetera)

– welche Daten man allgemein am eigenen Computer verarbeitet (Chrome OS und weitere Cloud-Computing-Angebote) et cetera

das Konto Chat-Konversationen (Kommunikationsinhalte) nicht mehr speichert. Bei Wahl der Option „vertraulich“ kann der Kommunikationspartner keine Konversationen mehr mit seinem Konto verknüpfen. Ähnlich sieht es bei Googles Voice aus, das bisher allerdings nur in den USA verfügbar ist: Hier lässt sich verhindern, dass Telefongespräche nach einer automatischen Spracherkennung im Konto landen.

Im Umgang mit Googles Toolbar lassen sich alle Funktionen, die automatisch URLs oder andere Informationen über besuchte Webseiten an die Firma senden beziehungsweise mit dem Konto verknüpfen, in den Einstellungen deaktivieren. Die erwähnte Webhistorie, die dienstübergreifende Suchanfragen standardmäßig mit dem Konto verknüpft, sollte man deaktivieren. Desgleichen die Option, ständig mit dem Konto angemeldet zu bleiben. Das DoubleClick-Cookie, mit dem Google dienstübergreifend persönliche Informationen für interessensbasierte Werbung erfasst, kann man auf der Firmenseite zu Werbung und Datenschutz dauerhaft abschalten (siehe *iX*-Link). Dort lassen sich außerdem bisher abgeleitete Interessen wieder entfernen.

Bei einigen Diensten, speziell den mobilen, sieht es bezüglich der Wahlmöglichkeiten momentan eher dürftig aus. So verweist Google bei Navigation, Goggles oder Sync lediglich auf die allgemeinen mobilen Nutzungs- und Datenschutzbestimmungen, und die wiederum sind nicht einmal in deutscher Sprache verfügbar. Mobile Dienste orten den Nutzer teilweise ständig. Android selbst ist standardmäßig so konfiguriert, dass es den Standort des Nutzers zu jeder Zeit an Google überträgt – was man wiederum per Einstellungen unterbinden kann, wie Abbildung 2 zeigt. Bei Deaktivierung bestimmter Optionen können Android Apps nicht mehr ohne Weiteres Standortdaten im Hintergrund übertragen. Der rechten Abbildung ist zu entnehmen, dass Optionen bestehen, den automatischen Datenaustausch zwischen Android-Apps und dem Internet zu verhindern.



Android-Einstellungen zur Lokalisierung (links) und Synchronisierung (Abb. 2)

Fazit

Alles in allem können Internetnutzer im Google-Umfeld viel für den Schutz ihrer persönlichen Daten tun, indem sie so wenig persönliche Daten wie möglich mit dem Google-Konto verknüpfen. Man kann unter anderem alternative Dienste oder separate Konten verwenden. Zweitens sollten Surfer verhindern, dass Daten sich auf Basis von Cookies oder IP-Adressen korrelieren lassen. Hierzu bietet sich die Browserkonfiguration durch Plug-ins an.

Schließlich sollten die Datenschutzeinstellungen innerhalb der genutzten Dienste (Opt-out) sinnvoll gewählt sein. Der Anwender muss seine Wahlmöglichkeiten eben aktiv nutzen. Daran dürfte sich künftig nichts ändern. Immerhin erkennt Google an, „dass jeder seine eigene Einstellung zum Datenschutz hat“ und will „möglichst allen Nutzern gerecht“ werden – durch „sinnvolle und detaillierte Wahlmöglichkeiten“. So steht es in Googles Datenschutzprinzipien (siehe *iX*-Link), und eigene Untersuchungen bestätigen das. Der Kasten „Was Google alles über jeden wissen könnte“ listet eine Vielfalt an Daten auf, die die Mountain Viewer erfassen können.

Eine vollständige Abkehr von Google stellt aufgrund des Nutzwertes, der verpasst würde, keine wirkliche Alternative dar und ist aufgrund von Googles Präsenz im Internet wahrscheinlich unmöglich. Man denke nur an Analytics und Street View, in die man unwissentlich involviert werden kann. Einzelne Dienste hingegen sollte man jedoch gar nicht oder allenfalls mit dedizierten Google-Konten verwenden, denn hier steht der Mehrwert nicht im Verhältnis zu den damit verbundenen Risiken. Dazu zählen vor allem Checkout, Health und Latitude. (hb)

PROF. NORBERT POHLMANN

ist geschäftsführender Direktor des Instituts für Internet-Sicherheit und Professor an der FH Gelsenkirchen im Fachbereich Informatik der Vertiefungsrichtung Internet und mobile Netze.

NIKOLAI SPOGAHN

studiert an der FH Gelsenkirchen im Masterstudiengang Angewandte Informatik mit dem Schwerpunkt Kommunikationstechnik und Internet.

Literatur

[1] Nikolai Spogahn; Google – die zwei Seiten des mächtigen Internet-Konzerns; Studie des Instituts für Internet-Sicherheit der Fachhochschule Gelsenkirchen, 2011; PDF im *iX*-Link

[2] Norbert Pohlmann; Cloud Computing – European perspective; RSA-Workshop während der RSA-Konferenz 2011, San Fancisco, USA; PDF im *iX*-Link

[3] Bernhard Carsten Witt; Datenschutz kompakt und verständlich; Eine praxisorientierte Einführung; Wiesbaden (Vieweg+Teubner) 2007

Alle Links: www.ix.de/ix1107098