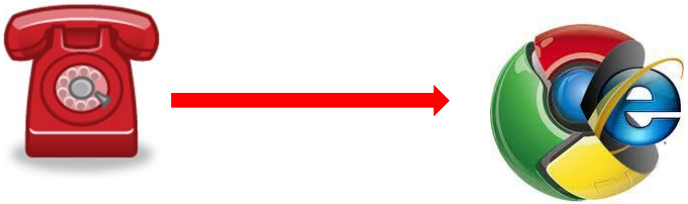
Smartphone-, Tablet-Nutzung und Datenschutz

Fachtagung für Multiplikatorinnen und Multiplikatoren

17. März 2015

Technik

Handy:
Telefon mit dem auch im Internet surfen kann



Smartphone/Tablet
Computer mit dem man auch telefonieren kann

Typische Merkmale

- Smartphones sind nicht für das Telefonieren optimiert, sondern für viele andere Funktionen
- Es hat in der Regel keine Tastatur, sondern ein Touchscreen
- Smartphones verfügen über ein Betriebssystem
- Es ermöglicht Programme von Drittherstellern zu installieren
- Kann sowohl Standard-Webseiten als auch mobil optimierte Webseiten darstellen.
- Eine schnelle Internet-Anbindung erfolgt mittels mobilem Breitband und WLAN
- Geht z.B. für Aktualisierungen ungefragt ins Internet
- Smartphones verfügen oft über unterschiedliche Sensoren. Hierzu zählen z.B. Bewegungssensoren, akustische oder optische Sensoren, sowie GPS-Empfänger.

Technik

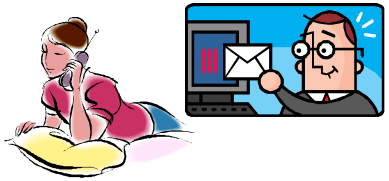
Smartphones haben genau wie Computer Betriebssysteme
(OS = Operating System)


IOS von Apple


Android, von der Open Handset Alliance (unter der Leitung von Google) entwickelt


BlackBerry OS von RIM


Windows Phone von Microsoft

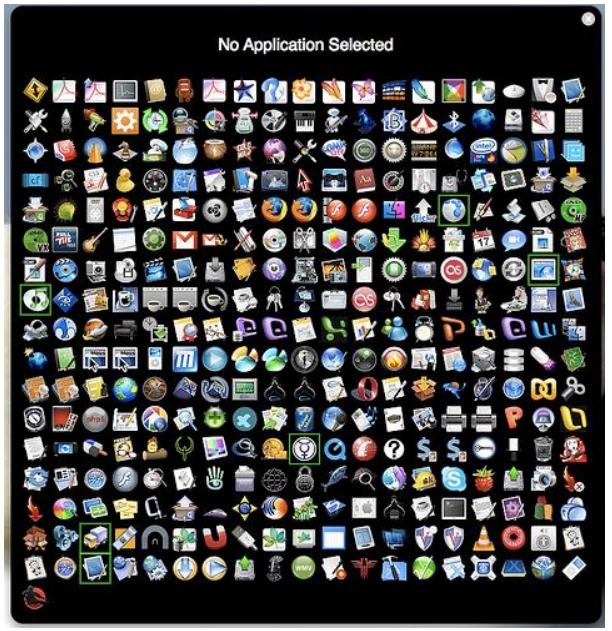


Funktionen

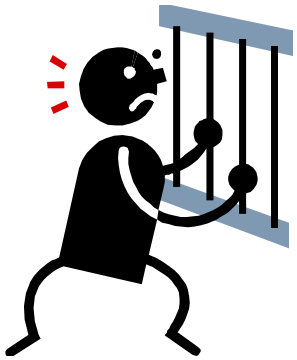
- **Kommunikationszentrale** Mobiltelefon, Webbrowser, E-Mail, SMS, MMS sowie IP-Telefonie (VoIP), Instant Messaging (IM) und Chat, teilweise auch Fax, Video-Telefonie und Konferenz-Lösungen
- **Personal Information Manager (PIM)** mit Adressbuch, Terminkalender, Aufgabenliste, Notizblock, Geburtstagsliste usw. mit Abgleich mit einer Desktop-Applikation oder über das Internet
- **Diktiergerät**
- **Datenspeicher**
- **Medienfunktionen** mit Mediaplayer, Radio, Bildbetrachter, Foto- und Videokamera
- **Taschencomputer** beispielsweise Textverarbeitung, Tabellenkalkulation, PDF-Reader, Taschenrechner usw.
- **Funk-Modem** für den PC, auch Tethering genannt
- **Navigation** mit Navigationssystem und Landkarten für andere standortbezogene Dienste (Location Based) wie mobile Umgebungssuche
- **Spiele-Plattform/mobile Spielkonsole**

Apps

- App steht für „Application“, auf deutsch „Anwendungen“
- Apps sind kleine Programme, die auch zusätzlich auf dem Smartphone installiert werden können
- Diese Apps werden über Vertriebsplattform angeboten und können von dort kostenlos oder kostenpflichtig heruntergeladen werden.
- Stores (Beispiele):
  - App Store von Apple (I-Tunes)
  - Google Play für Android
  - Windows Phone Store von Microsoft
  - Blackberry Apps World



http://litflow.de/magazin/wp-content/uploads/2012/09/apps1.jpg



„Gefängnisausbruch……“

- **Jailbreak** (engl: Gefängnisausbruch) bezeichnet das Entfernen von Nutzungsbeschränkungen bei Smartphones, die durch den Hersteller entsprechend gesperrt sind. Der Begriff entstand ursprünglich bzgl. Apple-Geräten, bei Geräten mit Android-Betriebssystem ist eher der Begriff **Rooten** gebräuchlich.

- Mittels entsprechender Software wird das Betriebssystem modifiziert, damit bisher gesperrte Funktionen freigeschaltet werden oder zusätzliche Software auf dem Gerät installiert werden kann (z.B. Apps aus anderen Quellen)
- Kann zum Verlust der Gewährleistung oder Garantie führen

In-App-Käufe

- Viele Apps sind kostenlos
- Bei kostenlosen Apps – Werbeeinblendungen
- Premiumversion ohne Werbung kostenpflichtig
- Premiumversion kann aus der App heraus bestellt werden (In-App-Kauf)
- In-App-Käufe von „Spiele-Zubehör“

In-App-Käufe

- In-App-Produkte 0,83 € bis 74,99 € pro Artikel


38,890
19
0
NOT ENOUGH COINS!
Oh Darn! You don't have enough Coins!
41,000
36,000
for 8,99 €
BUY COINS
Paul
211,000
Wenqi
176,000
Bronwen
141,000
EARN
+40
You
133,050
Yeti Shop
Amulett der Streifen
35,99 €

Smartphones und Apps – die Spione in der Hosentasche

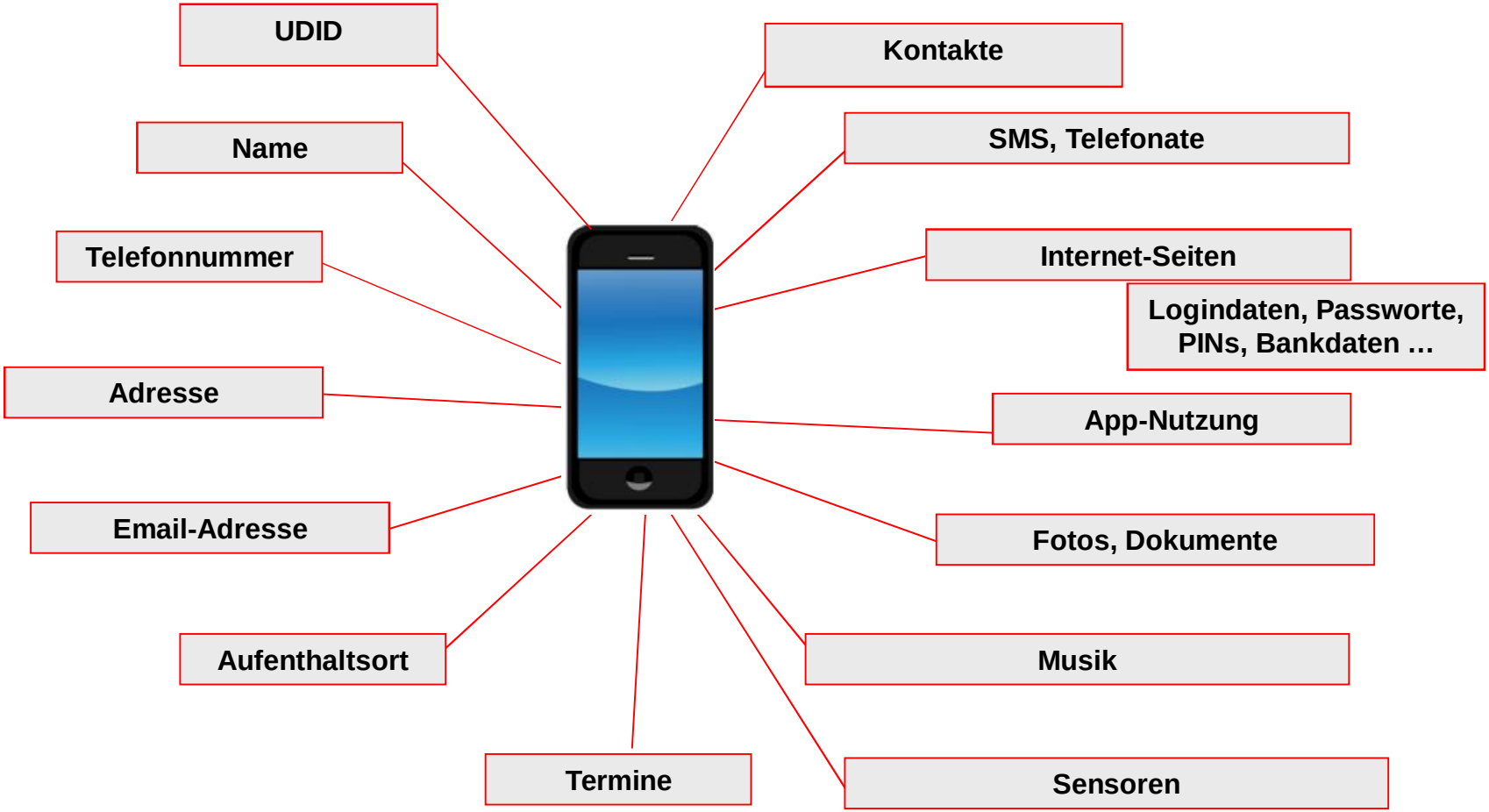
Smartphones und Tablets speichern eine Vielzahl persönlicher Nutzerdaten.

Wichtige Fragen sind daher:

- Was weiß mein Smartphone über mich und woher?
- Wer erhält die Daten und warum?
- Was kann ich dagegen tun?

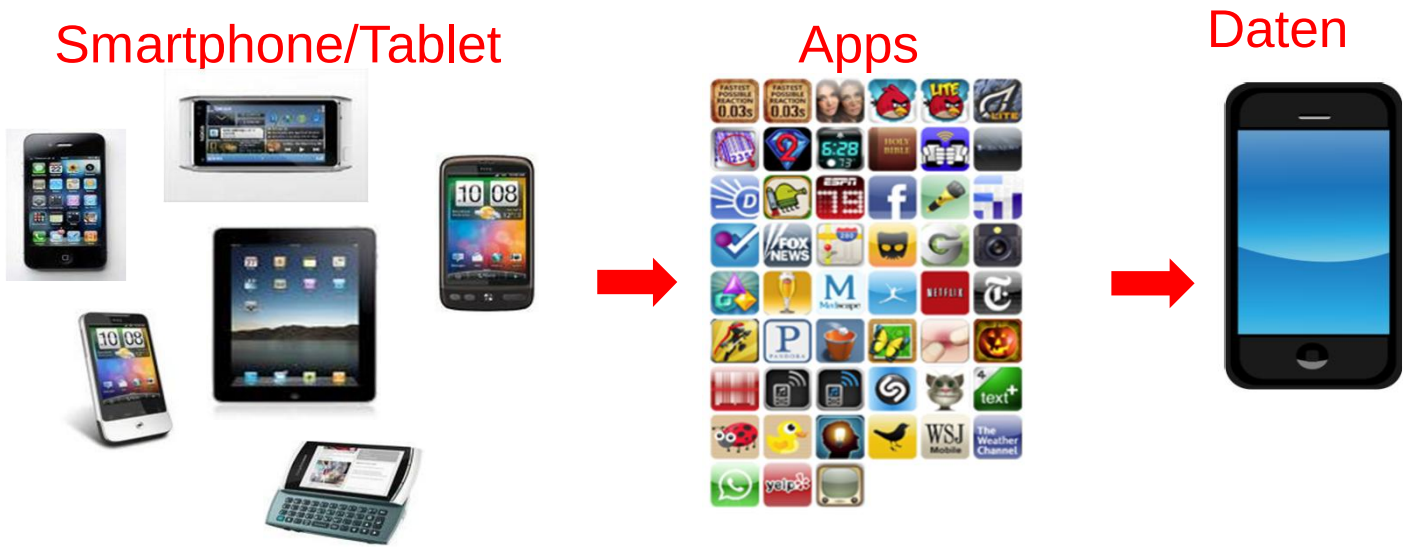
UDID = Unique Device Identification Number

Was weiß mein Smartphone über mich ?



UDID = Unique Device Identification Number

- Eine einmalige Nummer die bei der Installation des Geräts vergeben wird
- Kann nur durch eine Neuinstallation des Betriebssystems geändert werden.
- Wird die Nummer noch mit einer Registrierung verbunden und an Dritte, z.B. Werbenetzwerke, weitergegeben, ist ein dauerhaftes personenbezogenes Tracking möglich.
- Nutzer haben im Regelfall weder Kenntnis von der Weitergabe, noch können sie dieser Nutzung widersprechen.



Bei Smartphones verarbeiten sowohl die Betriebssysteme personenbezogenen Daten als auch die auf den Geräten installierten Anwendungen (Apps).

UDID = Unique Device Identification Number

Datenzugriffe durch Apps

UDID #7411-0815

- gerätespezifisch
- weltweit eindeutig
- dauerhaft vergeben

Ein Fingerabdruck – aber zunächst meist anonym.

Anmeldung:

ID: donald@duck.com
PW: d0na1d

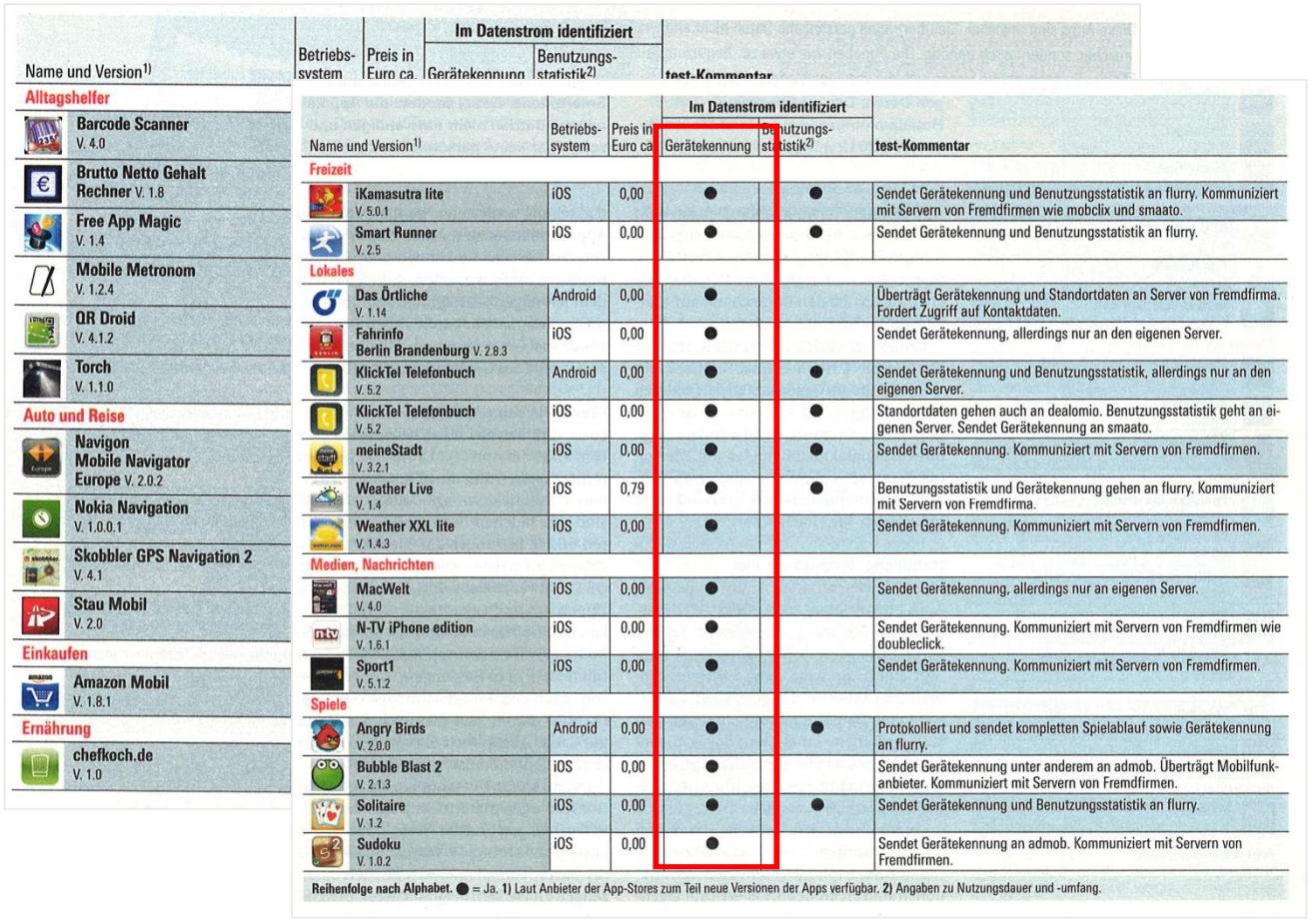
UDID # 4711-0815

facebook

Quelle: skibb-duck.deviantart.com

UDID = Unique Device Identification Number

Datenzugriffe durch Apps



Name und Version[1]	Betriebssystem	Preis in Euro ca.	Im Datenstrom identifiziert: Gerätekennung	Im Datenstrom identifiziert: Benutzungsstatistik[2]	test-Kommentar
Freizeit					
iKamasutra lite V. 5.0.1	iOS	0,00	●	●	Sendet Gerätekennung und Benutzungsstatistik an flurry. Kommuniziert mit Servern von Fremdfirmen wie mobclix und smaato.
Smart Runner V. 2.5	iOS	0,00	●	●	Sendet Gerätekennung und Benutzungsstatistik an flurry.
Lokales					
Das Örtliche V. 1.14	Android	0,00	●		Überträgt Gerätekennung und Standortdaten an Server von Fremdfirma. Fordert Zugriff auf Kontaktdaten.
Fahrinfo Berlin Brandenburg V. 2.8.3	iOS	0,00	●		Sendet Gerätekennung, allerdings nur an den eigenen Server.
KlickTel Telefonbuch V. 5.2	Android	0,00	●	●	Sendet Gerätekennung und Benutzungsstatistik, allerdings nur an den eigenen Server.
KlickTel Telefonbuch V. 5.2	iOS	0,00	●	●	Standortdaten gehen auch an dealomio. Benutzungsstatistik geht an eigenen Server. Sendet Gerätekennung an smaato.
meineStadt V. 3.2.1	iOS	0,00	●	●	Sendet Gerätekennung. Kommuniziert mit Servern von Fremdfirmen.
Weather Live V. 1.4	iOS	0,79	●	●	Benutzungsstatistik und Gerätekennung gehen an flurry. Kommuniziert mit Servern von Fremdfirma.
Weather XXL lite V. 1.4.3	iOS	0,00	●		Sendet Gerätekennung. Kommuniziert mit Servern von Fremdfirmen.
Medien, Nachrichten					
MacWelt V. 4.0	iOS	0,00	●		Sendet Gerätekennung, allerdings nur an eigenen Server.
N-TV iPhone edition V. 1.6.1	iOS	0,00	●		Sendet Gerätekennung. Kommuniziert mit Servern von Fremdfirmen wie doubleclick.
Sport1 V. 5.1.2	iOS	0,00	●		Sendet Gerätekennung. Kommuniziert mit Servern von Fremdfirmen.
Spiele					
Angry Birds V. 2.0.0	Android	0,00	●	●	Protokolliert und sendet kompletten Spielablauf sowie Gerätekennung an flurry.
Bubble Blast 2 V. 2.1.3	iOS	0,00	●		Sendet Gerätekennung unter anderem an admob. Überträgt Mobilfunkanbieter. Kommuniziert mit Servern von Fremdfirmen.
Solitaire V. 1.2	iOS	0,00	●	●	Sendet Gerätekennung und Benutzungsstatistik an flurry.
Sudoku V. 1.0.2	iOS	0,00	●		Sendet Gerätekennung an admob. Kommuniziert mit Servern von Fremdfirmen.

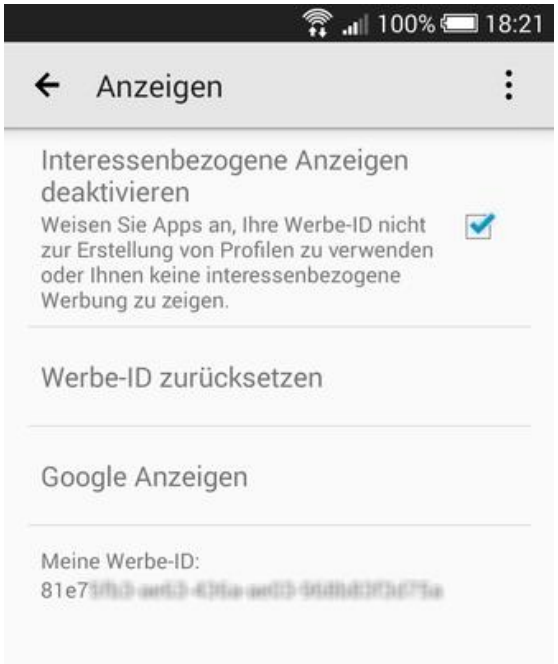
Reihenfolge nach Alphabet. ● = Ja. 1) Laut Anbieter der App-Stores zum Teil neue Versionen der Apps verfügbar. 2) Angaben zu Nutzungsdauer und -umfang.

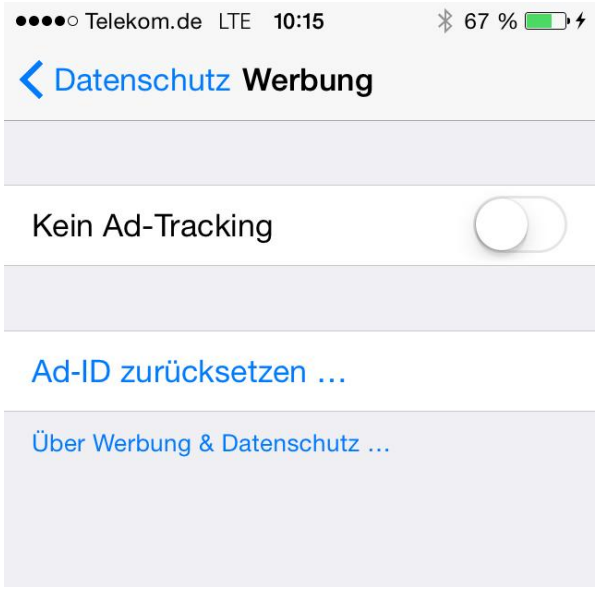
Quelle: Stiftung Warentest, Test 6/2012

Werbe-ID

- Apple untersagte bereits Anfang 2012 die Nutzung der einmalige UDID und führte für Werbezwecke und neue Advertising-ID ein
- Diese Nummer kann seitdem durch den Nutzer verwaltet und zurückgesetzt werden. (unter Einstellungen/Datenschutz/Werbung)
- Google hat seit August 2014 ebenfalls eine eigene Werbe-ID für Android eingeführt. (unter Einstellungen/Konto/Google/Anzeigen)

http://www.datenschutzkanzlei.de/2014/10/01/tracking-auf-smartphones-was-die-werbe-id-%C3%BCber-nutzer-ver%C3%A4t/





Zugriff auf Kontaktdaten

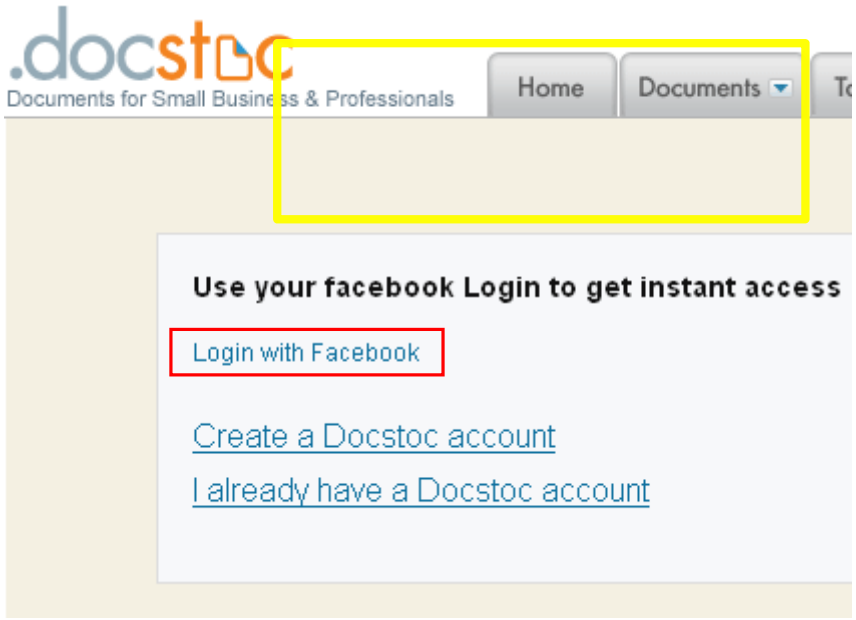
Übertragung und Speicherung von

- Adressen
- eMail-Adressen
- Telefonnummern

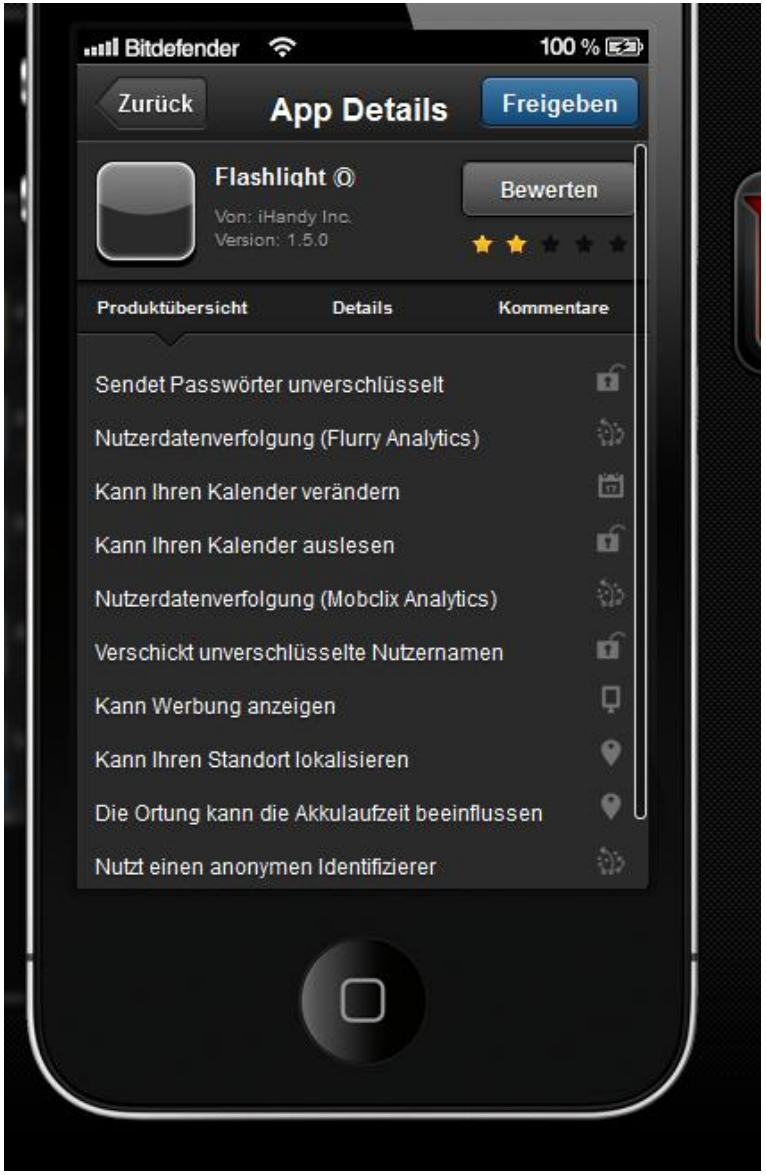
Häufig ohne Rückfrage oder Information der Nutzer !

Nutzer übermittelt Daten der Freunde und Bekannten an einen Dritten ohne Einverständnis der Freunde und Bekannten

Datenzugriff „über Bande“



http://cluefulapp.com/



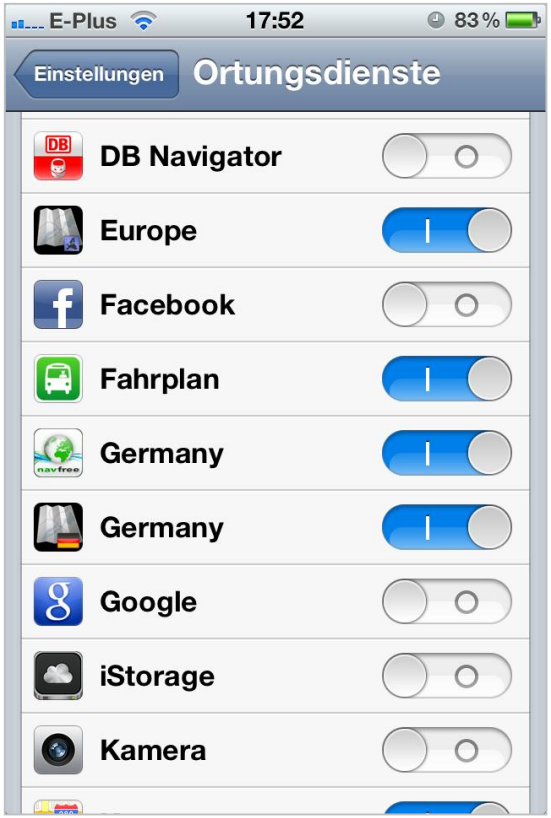
Standort

- **GPS (Satellit)**
  Es muss eine Sichtverbindung zu den Satelliten vorhanden sein, wodurch die Positionsbestimmung in Gebäuden nur ungenau möglich ist..
- **WLAN**
  Das Prinzip besteht darin, dass man anhand von mehreren Hot-Spots seine Position bestimmen kann. Dazu muss die Lage der Hotspots bekannt sein, die von verschiedenen Unternehmen erfasst wird. Das Smartphone kann dann ermitteln, welche Hot-Spots momentan empfangbar sind und berechnet mit Hilfe der Datenbanken den eigenen Standort.
- **GSM**
  Die Position eines Mobiltelefons ist für den Mobilfunkbetreiber durch die permanente Anmeldung am Netz in gewissen Genauigkeitsgrenzen bekannt. Bei der GSM-abhängigen Lokalisierung wird abgefragt, in welcher Funkzelle sich das Telefon zuletzt eingeklinkt hat.

Standort

- Bei **Apple** können Apps nur auf den Standort zugreifen, wenn man es ihnen erlaubt
- Man kann die Ortung für einzelne Dienste festlegen oder Ortungsdienste ganz deaktivieren
- Unter Datenschutz/Ortungsdienste kann man einsehen, welche Apps auf den Standort zugegriffen haben
- **Android**-Apps zeigen bei der Installation an, ob auf den Standort zugegriffen wird
- Die eingeräumten Berechtigungen können unter „Einstellungen/Apps“ eingesehen werden

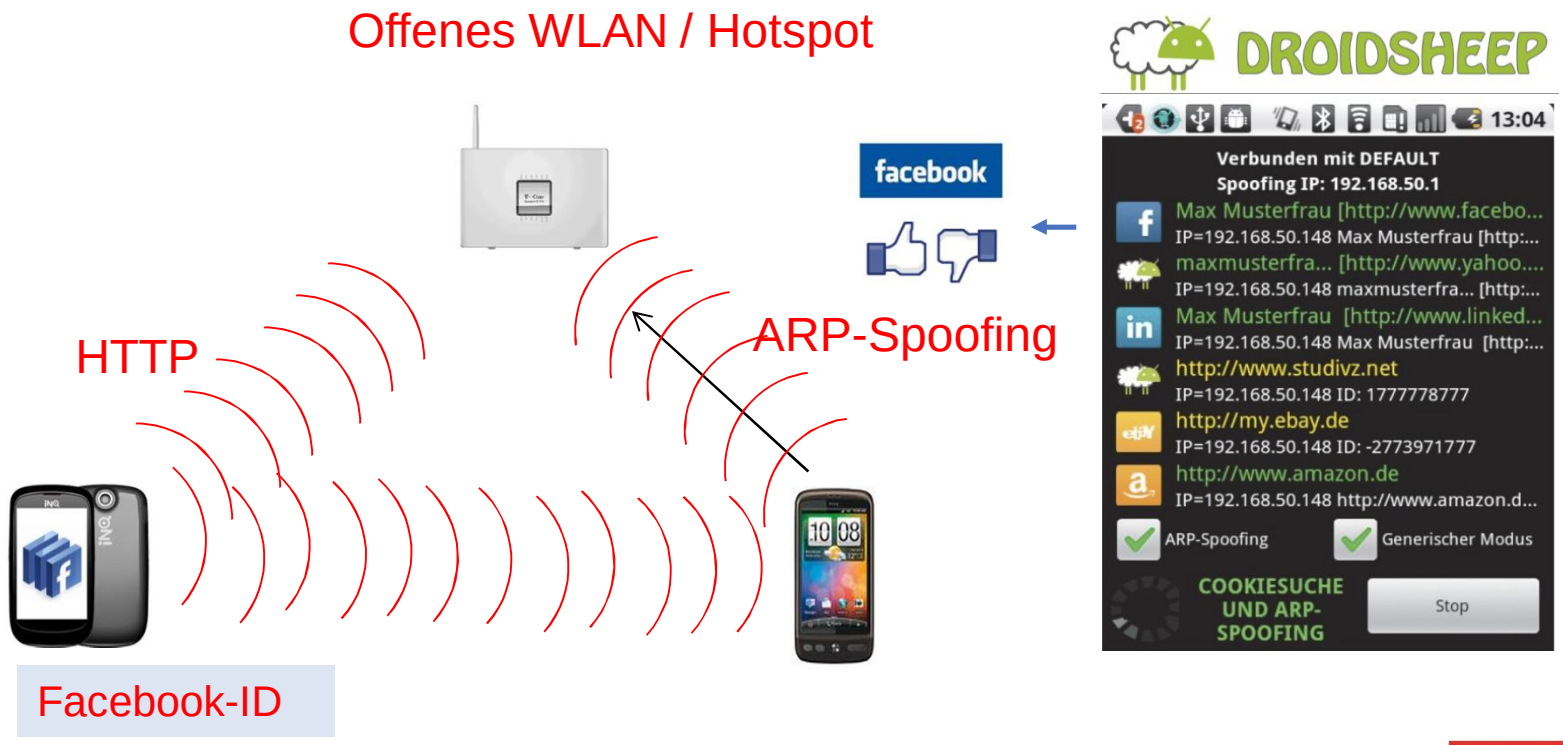
iPhone – iOS 4/5 Standortdaten



iPhone – iOS 6 Datenschutz

Datenzugriff in offenen WLAN-Netzen/Hotspots

ARP-Spoofing: Kommt von to spoof – dt. täuschen, reinlegen, insgesamt zu übersetzen mit Anfrageverfälschung
Der Datenverkehr kann abgehört oder manipuliert werden.



Vorsätzliche Datenspionage

lookout
MOBILE SECURITY

Desktop-Wechsel-App

Telefonnummer
Nutzerdaten

Datenspuren vermeiden

- GPS-Funktion nach Bedarf aktivieren
- WLAN-Funktion nach Bedarf aktivieren
- Datenanforderung bei Installation beachten
- Datenfreigaben bewusst erteilen

Schutz vor Schadsoftware

- Jeder Nutzer sollte sein Smartphone vor Verlust und Schadprogrammen schützen.
- Auf iPhones sind Sicherheitsprogramme Standard.
- Android-Nutzer sollten Sicherheits-Apps installieren.
- **McAfee** schützt das Smartphone am besten bei Verlust und vor Schadprogrammen. Die App kostet 30 Euro im Jahr.
- Kostenlos sichert dagegen **Avast!** das Smartphone.
- Doch selbst mit Sicherheitsprogramm gilt: Laden Sie keine Apps aus inoffiziellen Stores und meiden Sie dubiose Internetseiten.

test

Sicherheits-Apps

Kein Zugriff für Gauner

Sicherheits-Apps Smartphones sind zunehmend Ziel von Kriminellen. Apps helfen bei Verlust und schützen vor Schadsoftware.

Life companion, Lebensgefährte, nennt Samsung sein neues Smartphone Galaxy S4 – das ist nicht einmal übertrieben. Für viele Menschen ist ihr Handy ein unverzichtbarer Begleiter: Es kennt die Telefonnummern von Freunden und Kollegen, zeigt E-Mails an und merkt sich Passwörter, etwa für WLan-Netze. Besondere Momente hält es als Foto oder Video fest. Fürs Onlineshopping hat es sogar die Kreditkartendaten gespeichert.

Umso schlimmer, wenn dieser Lebensgefährte abhanden kommt, Geheimnisse ausplaudert oder sich mit Krankheiten infiziert. Um das zu verhindern gibt es kleine Programme, Apps, die Smartphones schützen sollen. Wir haben 15 Sicherheits-Apps für Handys getestet, die das Betriebssystem Android verwenden (für iPhones ▸

Unser Rat

Jeder Nutzer sollte sein Smartphone vor Verlust und Schadprogrammen schützen. Auf iPhones sind Sicherheitsprogramme Standard. Android-Nutzer sollten Sicherheits-Apps installieren. **McAfee** schützt das Smartphone am besten bei Verlust und vor Schadprogrammen. Die App kostet 30 Euro im Jahr. Kostenlos sichert dagegen **Avast!** das Smartphone. Doch selbst mit Sicherheitsprogramm gilt: Laden Sie keine Apps aus inoffiziellen Stores und meiden Sie dubiose Internetseiten.

7/2013 test

Handy suchen

- Um das iPhone orten zu können, loggt man sich an einem Computer in seinen iCloud-Account ein.
- iCloud ortet nun alle iOS-Geräte bis auf wenige Meter genau, selbst wenn diese ausgeschaltet sind.
- Des Weiteren hat man die Möglichkeit, das Handy einen Signalton in voller Lautstärke abspielen zu lassen.
- Auch kann man eine Nachricht auf das Display des Handys schicken oder dieses aus der Ferne sperren. Diese Funktionen sind allerdings nur bei einem eingeschalteten Handy nutzbar.

Wichtige Tipps

- Verwenden Sie nur Apps aus sicheren Quellen, also den Softwareportalen der Geräte- bzw. Betriebssystemhersteller.
- Machen Sie sich mit den besonderen Datenschutzbestimmungen einer App vertraut. Beachten Sie, dass diese sich jederzeit ändern können.
- Nutzen Sie die Datenschutzeinstellungen, um ungewollte Datenübertragungen einzuschränken; Bluetooth, GPS und WLAN sollten nur aktiviert sein, wenn sie benötigt werden.
- Achten Sie darauf, welche Daten Sie auf Ihrem Smartphone gespeichert und abrufbar haben.
- Schützen Sie Ihre Daten durch Verschlüsselung, Passwort und gegebenenfalls die Löschfunktion nach Verlust.
- Löschen Sie Ihre Daten, bevor Sie das Smartphone zur Reparatur geben oder verkaufen.
- Virenschutz und Firewall sind beim Smartphone unbedingt zu empfehlen – auch wenn ihr Schutz nicht dem beim heimischen PC entspricht.
- Führen Sie Sicherheitsupdates durch und aktualisieren Sie regelmäßig das Betriebssystem.
- Sofern Sie wissen, wer Ihre Daten verwaltet, können Sie sich an diesen Anbieter wenden und Auskunft über die gespeicherten Daten fordern.

„analoge“ Datenspuren entfernen

- Sperrcode
  ….entsperren bei Android durch wischen